Gröbner Bases & their Computation

Definitions + First Results

Priyank Kalla

Professor
Electrical and Computer Engineering, University of Utah
kalla@ece.utah.edu
http://www.ece.utah.edu/~kalla

Slides updated Oct 22, 2019

Agenda:

- Now that we know how to perform the reduction $f \xrightarrow{F=\{f_1,\ldots,f_s\}}_+ r$
- Study Gröbner Bases (GB)
  - Motivate GB through ideal membership testing
  - Study how they are related to ideal of leading terms
  - Study various definitions of GB
  - Study Buchberger's S-polynomials and the Buchberger's algorithm to compute GB
- Minimal and Reduced GB
- Application to ideal membership testing

From the last lecture: Multivariate Division Algorithm

Inputs: $f, f_1, \dots, f_s \in \mathbb{F}[x_1, \dots, x_n], f_i \neq 0$
Outputs: $u_1, \dots, u_s, r$ s.t. $f = \sum f_i u_i + r$ where r is reduced w.r.t. $F = \{f_1, \dots, f_s\}$ and $\max(lp(u_1)lp(f_1), \dots, lp(u_s)lp(f_s), lp(r)) = lp(f)$

$u_i \leftarrow 0$; $r \leftarrow 0$, $h \leftarrow f$
while $(h \neq 0)$ **do**
  if $\exists i$ s.t. $lm(f_i) \mid lm(h)$ **then**
    choose i least s.t. $lm(f_i) \mid lm(h)$
    $u_i = u_i + \frac{lt(h)}{lt(f_i)}$
    $h = h - \frac{lt(h)}{lt(f_i)} f_i$
  else
    $r = r + lt(h)$
    $h = h - lt(h)$
  end if
end while

Algorithm 1: Multivariate Division of f by $F = \{f_1, \dots, f_s\}$

Let $F = \{f_1, \ldots, f_s\}; \quad J = \langle f_1, \ldots, f_s \rangle$ and let $f \in J$. Then we should be able to represent $f = u_1 f_1 + \cdots + u_s f_s + r$ where $r = 0$. If we were to divide f by $F = \{f_1, \ldots, f_s\}$, then we will obtain an intermediate remainder (say, h) after every one-step reduction. Note $h \in J$ because $f, f_1, \ldots, f_s$ are all in J. The leading term of every such remainder ($\mathrm{LT}(h)$) should be divisible by the leading term of at least one of the polynomials in F. Only then we will have $r = 0$.

Definition

Let $F = \{f_1, \ldots, f_s\}; \; G = \{g_1, \ldots, g_t\}$;
$J = \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$. Then G is a **Gröbner Basis** of J

$$\iff$$

$$\forall f \in J \;\; (f \neq 0), \quad \exists i : \mathrm{lm}(g_i) \mid \mathrm{lm}(f)$$

Definition

$G = \{g_1, \ldots, g_t\} = GB(J) \iff \forall f \in J, \exists g_i \text{ s.t. } lm(g_i) \mid lm(f)$

As a consequence of the above definition:

Definition

$G = GB(J) \iff \forall f \in J, f \xrightarrow{g_1, g_2, \cdots, g_t}_+ 0$

- Implies a "decision procedure" for ideal membership
- To check if $f \in \langle f_1, \ldots, f_s \rangle$:
- Compute $GB(f_1, \ldots, f_s) = G = \{g_1, \ldots, g_t\}$
- Reduce $f \xrightarrow{g_1, \ldots, g_t}_+ r$, and check if $r = 0$

Understanding GB through some examples

- $J = \langle f_1, f_2 \rangle \subset \mathbb{Q}[x, y]$, DEGLEX $y > x$
- $f_1 = yx - y, \quad f_2 = y^2 - x$ and let $f = y^2x - x$
- $f = yf_1 + f_2$ so $f \in J$
- Apply division: i.e. REDUCE $f \xrightarrow{f_1, f_2}_+ r_1$
- Solve it in classroom: $r_1 = 0$
- Now try: $f \xrightarrow{f_2, f_1}_+ r_2 = x^2 - x$
- Does there exist f_i s.t. $lm(f_i) \mid lm(r_2)$?
- $G = \{f_1, f_2, x^2 - x\}$ is a GB. Why?

It has got to do with Leading Monomials

- Let $f \in J = \langle f_1, f_2 \rangle$: so $f = h_1 f_1 + h_2 f_2$
- Consider only leading terms:
- If $lt(f) \in \langle lt(f_1), lt(f_2) \rangle$, then some $lm(f_i) \mid lm(f)$ [observe: this has to be true!]
- But, what if $lt(f) \notin \langle lt(f_1), lt(f_2) \rangle$?
- Refer to the example on the previous slide

It has got to do with Leading Monomials

- Let $f \in J = \langle f_1, f_2 \rangle$: so $f = h_1 f_1 + h_2 f_2$
- Consider only leading terms:
- If $lt(f) \in \langle lt(f_1), lt(f_2) \rangle$, then some $lm(f_i) \mid lm(f)$ [observe: this has to be true!]
- But, what if $lt(f) \notin \langle lt(f_1), lt(f_2) \rangle$?
- Refer to the example on the previous slide

Cancellation of Leading Terms

When f is a polynomial combination of (say) $h_i f_i + h_j f_j$, such that the leading terms of $h_i f_i$ and $h_j f_j$ cancel each other, then $lt(f) \notin \langle lt(f_i), lt(f_j) \rangle$.
When does this happen?
This happens when the leading term of some combination of f_i, f_j $(ax^\alpha f_i - bx^\beta f_j)$ cancel!

Buchberger's S-polynomial

$S(f, g) = \frac{L}{lt(f)} \cdot f - \frac{L}{lt(g)} \cdot g$

- $L = \text{LCM}\,(lm(f), lm(g))$
- How to compute LCM of leading monomials?

Let $\text{multideg}(f) = X^{\alpha}, \text{multideg}(g) = X^{\beta}$, where $X^{\alpha} = x_1^{\alpha_1} \dots x_n^{\alpha_n}$, and let $\gamma = (\gamma_1, \dots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$. Then the $x^{\gamma} = \text{LCM}(\text{lm}(f),$ $\text{lm}(g))$.

Buchberger's S-polynomial

$S(f, g) = \frac{L}{lt(f)} \cdot f - \frac{L}{lt(g)} \cdot g$

- $L = \text{LCM}\left(lm(f), lm(g)\right)$
- How to compute LCM of leading monomials?

Let $\text{multideg}(f) = X^\alpha, \text{multideg}(g) = X^\beta$, where $X^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$, and let $\gamma = (\gamma_1, \dots, \gamma_n)$, where $\gamma_i = \max(\alpha_i, \beta_i)$. Then the $x^\gamma = \text{LCM}(\text{lm}(f), \text{lm}(g))$.

This S-polynomial (S = syzygy) cancels $lt(f), lt(g)$, gives a polynomial $h = S(f, g)$ with a new $lt(h)$.

This S-polynomial with a new $lt()$ is the missing piece of the GB puzzle!

Understanding S-poly some more...

- While S-poly gives new $lt(h)$, it may still have some redundant information
- $f = x^3y^2 - x^2y^3; \quad g = 3x^4 + y^2$
- $Spoly(f, g) = -x^3y^3 + x^2 - \frac{1}{3}y^3$
- x^3y^3 can be composed of $lt(f)$
- Reduce: $Spoly(f, g) \xrightarrow{f,g}_+ r$
- IN this case: $r = -x^2y^4 - 1/3y^3$
- If $r \neq 0$ then r provides "new information" regarding the basis

Theorem (Buchberger's Theorem [1])

Let $G = \{g_1, \ldots, g_t\}$ be a set of non-zero polynomials in $\mathbb{F}[x_1, \ldots, x_n]$. Then G is a Grobner basis for the ideal $J = \langle g_1, \ldots, g_t \rangle$ if and only if **for all** $i \neq j$

$$S(g_i, g_j) \xrightarrow{G}_+ 0$$

Theorem (Buchberger's Theorem [1])

Let $G = \{g_1, \dots, g_t\}$ be a set of non-zero polynomials in $\mathbb{F}[x_1, \dots, x_n]$. Then G is a Grobner basis for the ideal $J = \langle g_1, \dots, g_t \rangle$ if and only if **for all** $i \neq j$

$$S(g_i, g_j) \xrightarrow{G}_+ 0$$

Can you think of an algorithm to compute GB(J)?

Buchberger's Algorithm

INPUT : $F = \{f_1, \ldots, f_s\}$
OUTPUT : $G = \{g_1, \ldots, g_t\}$
$G := F$;
REPEAT
  $G' := G$
  For each pair $\{f, g\}, f \neq g$ in G' DO
    $S(f, g) \xrightarrow{G'}_+ r$
    IF $r \neq 0$ THEN $G := G \cup \{r\}$
UNTIL $G = G'$

$$S(f, g) = \frac{L}{lt(f)} \cdot f - \frac{L}{lt(g)} \cdot g$$

$L = \text{LCM}(lm(f), lm(g))$, $lm(f)$: leading monomial of f

With some more detail...

Inputs: $F = \{f_1, \ldots, f_s\} \subset \mathbb{F}[x_1, \ldots, x_n], f_i \neq 0$
Outputs: $G = \{g_1, \ldots, g_t\}$, a Gröbner basis for $\langle f_1, \ldots, f_s \rangle$

```
Initialize: G := F; 𝒢 := {{f_i, f_j} | f_i ≠ f_j ∈ G}
while 𝒢 ≠ ∅ do
    Pick a pair {f, g} ∈ 𝒢
    𝒢 := 𝒢 − {{f, g}}
    Spoly(f, g) →_+^G h
    if h ≠ 0 then
        𝒢 := 𝒢 ∪ {{u, h} | ∀u ∈ G}
        G := G ∪ {h}
    end if
end while
```

Algorithm 2: Buchberger's algorithm from [2]

- $F = \{f_1, f_2\} \in \mathbb{Q}[x, y]$, LEX $y > x$; $\quad f_1 = xy - x$; $\quad f_2 = -y + x^2$
- Run Buchberger's algorithm:
  - Polynomial Pair: there's only one $\{f_1, f_2\}$
  - $Spoly(f_1, f_2) = \frac{xy}{xy} f_1 - \frac{xy}{-y} f_2$
  - $Spoly(f_1, f_2) = xy - x - xy + x^3 = x^3 - x \neq 0$
  - $Spoly(f_1, f_2) \xrightarrow{f_1, f_2}_+ x^3 - x$
  - New basis: $\{f_1, f_2, f_3 = x^3 - x\}$
  - New pairs: $\{f_1, f_3\}, \{f_2, f_3\}$
- $Spoly(f_1, f_3) \xrightarrow{f_1, f_2, f_3}_+ = yx - x^3 \xrightarrow{f_1, f_2, f_3}_+ 0$
- $Spoly(f_2, f_3) \xrightarrow{f_1, f_2, f_3}_+ 0$
- No more polynomial pairs remaining, so f_1, f_2, f_3 is the GB

- $F = \{f_1, f_2\} \in \mathbb{Q}[x, y]$, DEGLEX $x > y$; $f_1 = xy - x$; $f_2 = -y + x^2$
- Then: $f_1 = xy - x$; $f_2 = x^2 - y$
- $Spoly(f_1, f_2) \xrightarrow{f_1, f_2}_+ = -x^2 + y^2 \xrightarrow{f_1, f_2}_+ y^2 - y = f_3$;
- $Spoly(f_1, f_3) \xrightarrow{f_1, f_2, f_3}_+ = 0$
- $Spoly(f_2, f_3) \xrightarrow{f_1, f_2, f_3}_+ = 0$

A more interesting example

- $f_1 = x^2 + y^2 + 1; \quad f_2 = x^2y + 2xy + x$ in $\mathbb{Z}_5[x, y]$ LEX $x > y$
- $S(f_1, f_2) \xrightarrow{f_1, f_2}_+ f_3 = 3xy + 4x + y^3 + y$
- $\mathcal{G} := \{\{f_1, f_3\}, \{f_2, f_3\}\}$
- $G = \{f_1, f_2, f_3\}$
- $S(f_1, f_3) \xrightarrow{f_1, f_2, f_3}_+ f_4 = 4y^5 + 3y^4 + y^2 + y + 3$
- $\mathcal{G} := \{\cancel{\{f_1, f_3\}}, \{f_2, f_3\}, \{f_1, f_4\}, \{f_2, f_4\}, \{f_3, f_4\}\}$
- $G = \{f_1, \ldots, f_4\}$
- Now, all *Spoly* in $\mathcal{G}$ reduce to 0, so $GB = \{f_1, \ldots, f_4\}$

- Gröbner basis complexity is not very pleasant
- For $J = \langle f_1, \ldots, f_s \rangle \subseteq \mathbb{F}[x_1, \ldots, x_n]$: n variables, and let d be the degree of J
- Complexity of Gröbner basis
  - Degree of polynomials in G is bounded by $2(\frac{1}{2}d^2 + d)^{2^{n-1}}$ [3]
  - Doubly-exponential in n and polynomial in the degree d
- This is the complexity of the GB problem, not of Buchberger's algorithm – that's still a mystery
- In many practical cases, the behaviour is not that bad — but it is still challenging to overcome this complexity
- Our objective: to glean more information from circuits to overcome this complexity — we'll study these concepts a little later
- In general DEGREVLEX orders show better performance than LEX orders — but for Boolean circuits, our experience is slightly different

Minimal GB

A Gröbner basis $G = \{g_1, \dots, g_t\}$ is minimal if for all i, $\text{lc}(g_i) = 1$, and for all $i \neq j$, $\text{lm}(g_i)$ does not divide $\text{lm}(g_j)$.

- Obtain a minimal GB: Test if $lm(g_i)$ divides $lm(g_j)$, remove g_j. Then normalize the LC: Divide each g_i by $lc(g_i)$.
- Unfortunately, minimality is not unique
- Minimal GBs have same number of terms
- Minimal GBs have same leading terms

Make a GB minimal

- Over $\mathbb{Z}_5[x, y]$, LEX $x > y$

  A Gröbner basis:

$$
\begin{aligned}
f_1 &= x^2 + y^2 + 1 \\
f_2 &= x^2y + 2xy + x \\
f_3 &= 3xy + 4x + y^3 + y \\
f_4 &= 4y^5 + 3y^4 + y^2 + y + 3
\end{aligned}
$$

Make a GB minimal

- Over $\mathbb{Z}_5[x, y]$, LEX $x > y$

A Gröbner basis:

$$\begin{aligned} f_1 &= x^2 + y^2 + 1 \\ f_2 &= x^2y + 2xy + x \\ f_3 &= 3xy + 4x + y^3 + y \\ f_4 &= 4y^5 + 3y^4 + y^2 + y + 3 \end{aligned}$$

A minimal Gröbner basis:

$$\begin{aligned} f_1 &= x^2 + y^2 + 1 \\ \frac{f_3}{3} &= xy + 3x + 2y^3 + 2y \\ \frac{f_4}{4} &= y^5 + 2y^4 + 4y^2 + 4y + 2 \end{aligned}$$

A Reduced (Minimal) GB

A **reduced GB** for a polynomial ideal J is a GB G such that:

- $\text{lc}(p) = 1$, $\forall$ polynomials$p \in G$
- $\forall p \in G$, no monomial of p lies in $\langle \text{LT}(G - \{p\}) \rangle$.

In other words, no non-zero term in g_i, is divisible by any $\text{lm}(g_j)$, for $i \neq j$.

Reduced, minimal GB is a **unique, canonical representation of an ideal**!

To Reduce a Minimal GB, do the following:

- Compute a G.B. Make it minimal: remove g_i if $lp(g_j)$ divides $lp(g_i)$. Make all LC $= 1$.
- Reduce it: $G = \{g_1, \ldots, g_t\}$ is minimal G.B. Get $H = \{h_1, \ldots, h_t\}$:
  - $g_1 \xrightarrow{H_1}_+ h_1$, where h_1 is reduced w.r.t. $H_1 = \{g_2, \ldots, g_t\}$
  - $g_2 \xrightarrow{H_2}_+ h_2$, where h_2 is reduced w.r.t. $H_2 = \{h_1, g_3, \ldots, g_t\}$
  - $g_3 \xrightarrow{H_3}_+ h_3$, where h_3 is reduced w.r.t. $H_3 = \{h_1, h_2, g_4, \ldots, g_t\}$
  - $g_t \xrightarrow{H_t}_+ h_t$, where h_t is reduced w.r.t. $H_t = \{h_1, h_2, h_3, \ldots, h_{t-1}\}$
- Then $H = \{h_1, \ldots, h_t\}$ is a unique, minimal, reduced GB.

Reduce this minimal GB

$$
\begin{aligned}
f_1 &= x^2 + y^2 + 1 \\
f_2 &= xy + 3x + 2y^3 + 2y \\
f_3 &= y^5 + 2y^4 + 4y^2 + 4y + 2
\end{aligned}
$$

Reduce this minimal GB

$$
\begin{aligned}
f_1 &= x^2 + y^2 + 1 \\
f_2 &= xy + 3x + 2y^3 + 2y \\
f_3 &= y^5 + 2y^4 + 4y^2 + 4y + 2
\end{aligned}
$$

It is already reduced!

Example: Non-uniqueness of minimal GB

DEGLEX $y > x$ in $\mathbb{Q}[x, y]$:

$$\begin{aligned} f_1 &= y^2 + yx + x^2 \\ f_2 &= y + x \\ f_3 &= y \\ f_4 &= x^2 \\ f_5 &= x \end{aligned}$$

DEGLEX $y > x$ in $\mathbb{Q}[x, y]$:

$$\begin{aligned} f_1 &= y^2 + yx + x^2 \\ f_2 &= y + x \\ f_3 &= y \\ f_4 &= x^2 \\ f_5 &= x \end{aligned}$$

$\{f_3, f_5\}$ and $\{f_2, f_5\}$ are minimal GBs (non-unique)

Example: Non-uniqueness of minimal GB

DEGLEX $y > x$ in $\mathbb{Q}[x, y]$:

$$\begin{aligned} f_1 &= y^2 + yx + x^2 \\ f_2 &= y + x \\ f_3 &= y \\ f_4 &= x^2 \\ f_5 &= x \end{aligned}$$

$\{f_3, f_5\}$ and $\{f_2, f_5\}$ are minimal GBs (non-unique)
$\{f_3, f_5\}$ is a reduced GB

One (last) more definition of GB

Gröbner bases as ideals of leading terms

- Let $I = \langle f_1, \ldots, f_s \rangle$ be an ideal
- Denote by LT(I) the set of leading terms of all elements of I.
- $\text{LT(I)} = \{cx^\alpha : \exists f \in I \text{ with } \text{LT}(f) = cx^\alpha\}$
- $\langle LT(I) \rangle$ denotes the (monomial) ideal generated by elements of LT(I).

Contrast $\langle LT(I) \rangle$ with:

- $\langle lt(f_1), lt(f_2), \ldots, lt(f_s) \rangle$
- Is $\langle LT(I) \rangle = \langle lt(f_1), lt(f_2), \ldots, lt(f_s) \rangle$?
- Not always. Equality holds only when the set $\{f_1, \ldots, f_s\}$ is a Gröbner basis!

See this example....

- Let $f_1 = x^3 - 2xy; \quad f_2 = x^2y - 2y^2 + x$ DEGLEX $x > y$
- Note: $F = \{f_1, f_2\}$ is not a GB!
- $I = \langle f_1, f_2 \rangle$, and $x^2 = x \cdot f_2 - yf_1 \in I$
- $x^2 = lt(x^2) \in LT(I)$
- But, is $x^2 \in \langle lt(f_1), lt(f_2) \rangle$?
- Aside: BTW, what is a GB of a set of monomials?
- Compute $GB(f_1, f_2) = \{g_1 : 2y^2 - x, \quad g_2 : xy, \quad g_3 : x^2\}$
- Note that $\langle LT(I) \rangle = \{lt(g_1) = 2y^2, \; lt(g_2) = xy, \; lt(g_3) = x^2\}$

Definition

$G = \{g_1, \ldots, g_t\} \iff \langle lt(I) \rangle = \langle lt(g_1), \ldots, lt(g_t) \rangle$

Finally, to recap...

- Every ideal over $\mathbb{F}[x_1, \ldots, x_n]$ is finitely generated
- $J = \langle f_1, \ldots, f_s \rangle \subset \mathbb{F}[x_1, \ldots, x_n]$
- Every such ideal J has a Gröbner basis $G = \{g_1, \ldots, g_t\}$ which can always be computed
- $J = \langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$

Definition

$$G = \{g_1, \ldots, g_t\} = GB(J) \iff \forall f \in J, \exists g_i \text{ s.t. } lm(g_i) \mid lm(f)$$

Definition

$$G = GB(J) \iff \forall f \in J, f \xrightarrow{g_1, g_2, \cdots, g_t}_+ 0$$

Definition

$$G = \{g_1, \ldots, g_t\} = GB(J) \iff \langle lt(J) \rangle = \langle lt(g_1), \ldots, lt(g_t) \rangle$$

- Buchberger's algorithm computes Gröbner basis
- $Spoly(f, g) \xrightarrow{G}_{+} r$ cancels the leading terms of f, g and gives a polynomial with a new leading term
- A GB is computed when ALL $Spoly(f, g) \xrightarrow{G}_{+} 0$
- GB should be made minimal and then reduced
- Reduced GB = unique, canonical form (subject to the term order)
- GB as a decision procedure for ideal membership testing
  - Compute $G = GB(J)$, reduce $f \xrightarrow{G}_{+} r$, and check if $r = 0$

Definition (Ideal Membership Testing Algorithm)

$f \in J \iff f \xrightarrow{G}_{+} 0$ where $G = \{g_1, \dots, g_t\}$

Remainder modulo a Gröbner basis is unique, w.r.t. a given monomial order

- Fix a term order $>$, and let $G = \{g_1, \ldots, g_t\} = GB(J)$ be a Gröbner basis
- If $f \xrightarrow{G}_+ r_1$ and $f \xrightarrow{G}_+ r_2$, then $r_1 = r_2 = r$
- Then r is called the *normal form* of f modulo G: $r = \overline{NF(f)}^G$
- Then r is a unique canonical signature modulo a Gröbner basis

Extended Gröbner Basis

Let $F = \{f_1, \ldots, f_s\}, J = \langle F \rangle$ and compute $G = GB(J) = \{g_1, \ldots, g_t\}$ using Buchberger's algorithm. Then it is possible to extend Buchberger's algorithm to output not just G, but also a $t \times s$ matrix M with polynomial entries such that:

$$\begin{bmatrix} g_1 \\ g_2 \\ \vdots \\ g_t \end{bmatrix} = M \cdot \begin{bmatrix} f_1 \\ f_2 \\ \vdots \\ f_s \end{bmatrix} \tag{1}$$

Entries of M can be found by recording the "quotients of division" in Buchberger's algorithm. The "lift" command in Singular can solve that.

Extended Ideal Membership

- Let $F = \{f_1, \ldots, f_s\}, J = \langle F \rangle$ and compute $G = GB(J) = \{g_1, \ldots, g_t\}$
- Let $f \in J$, then we know that $f \xrightarrow{G}_+ r = 0$
- Then $f = h_1 g_1 + h_2 g_2 + \cdots + h_t g_t$
- From Eqn. (1) each g_i is some combination of $f_1, \ldots, f_s$
- Substitute g_i's: $f = u_1 f_1 + u_2 f_2 + \cdots + u_s f_s$

[1] B. Buchberger, "Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal," Ph.D. dissertation, University of Innsbruck, 1965.

[2] W. W. Adams and P. Loustaunau, *An Introduction to Gröbner Bases*. American Mathematical Society, 1994.

[3] T. W. Dube, "The Structure of Polynomial Ideals and Gröbner bases," *SIAM Journal of Computing*, vol. 19, no. 4, pp. 750–773, 1990.